CLAIMS

1. (currently amended) An apparatus for selectively processing first and second cryptographic hash algorithms, comprising:

a register file (12) having at least five registers for storing chaining variables;

a function circuit (22) receiving first (B), second (C) and third (D) chaining variables and an output that provides a logical data value;

a first multiplexer (24) having an input coupled to the register file for receiving a fourth (E) chaining variable and an output that provides the fourth chaining variable when the first cryptographic hash algorithm is being processed by the apparatus and ~~and~~ a zero value when the second cryptographic hash algorithm is being processed by the apparatus; and

a summing circuit (30) having a first input coupled to the output of the function circuit for receiving the logical data value, a second input coupled to the output of the first multiplexer, and an output coupled to the register file.

2. (previously presented) The apparatus of claim 1, further comprising:

a barrel shifter (40) having an input coupled to the output of the summing circuit;

an adder (41) having an input coupled to an output of the barrel shifter; and

a second multiplexer (42) having a first input coupled to the output of the summing circuit and a second input coupled to an output of the adder.

3. (previously presented) The apparatus of claim 2, further comprising:

a third multiplexer (26) having a first input coupled to the output of the second multiplexer (42) and a second input coupled to the register file (12) for receiving a fifth (A) chaining variable; and

a fourth multiplexer (28) having a first input coupled to the output of the second multiplexer and a second input coupled to the register file (12) for receiving the third (D) chaining variable.

4. (previously presented) The apparatus of claim 3, wherein the second multiplexer and the fourth multiplexer receive a signal that transfers a summed value from the output of the summing

circuit to the register file when the message digest hardware accelerator is processing an SHA-1 hash algorithm.

5. (previously presented) The apparatus of claim 3, wherein the second multiplexer and the third multiplexer receive a signal that transfers a summed value from the output of the barrel shifter to the register file when the message digest hardware accelerator is processing an MD5 hash algorithm.

6. (previously presented) The apparatus of claim 3, further comprising:

a first shift circuit (16) having an input coupled to the register file for receiving the first (B) chaining variable; and

a fifth multiplexer (14) having a first input coupled to an output of the first shift circuit, a second input coupled to the input of the first shift circuit and an output coupled to the register file for providing the second chaining variable.

7. (previously presented) The apparatus of claim 6, further comprising:

a second shift circuit (18) having an input coupled to the register file for receiving the fifth (A) chaining variable; and

a sixth multiplexer (20) having a first input coupled to an output of the second shift circuit, a second input coupled to the input of the second shift circuit and an output coupled to another input of the summing circuit.

8. (previously presented) A circuit for generating hash values in a first hash mode and a second hash mode, comprising:

a storage circuit (34, 36);

a register array (32) having registers for storing a message and an output for providing a round dependent data value (Wt);

a register file (12) for storing first (B), second (C), third (D), fourth (E) and fifth (A) chaining variables; and

an adder (30) having a first input coupled for receiving a first set of constant values stored in the storage circuit for the first hash mode and a second set of constant values for the second hash

mode, a second input coupled to the output of the register array, a third input coupled for receiving the fifth (A) chaining variable in the second hash mode and a shifted fifth chaining variable in the first hash mode, a fourth input coupled for receiving a logical function in accordance with the first, second and third chaining variables, and a fifth input coupled for receiving the fourth chaining variable in the second hash mode and a zero value in the first hash mode.

9 - 13. (canceled)

14. (previously presented) An apparatus integrated to provide a hash value of a variable length message in accordance with a first algorithm and a second algorithm, comprising:

a register file (12) having five registers preset to a first group of values for the first algorithm and to a second group of values for the second algorithm, the register file storing first (B), second (C), third (D), fourth (E) and fifth (A) chaining variables;

a function circuit (22) receiving first, second and third chaining variables and generating a first logical data value for the first algorithm and a second logical data value for the second algorithm;

a storage element (34, 36) for supplying a first set of constant values for the first algorithm and a second set of constant values for the second algorithm; and

a summing circuit (30) having a first input coupled to the output of the function circuit (22) and a second input coupled to the storage element for receiving one of the first and second sets of constant values.

15. (previously presented) The apparatus of claim 14, further including a register array (32) having a decoder circuit (120) and a plurality of registers for selecting a data word stored in one of the plurality of registers and supplying the data word to an output of the register array when computing the first algorithm.

16. (previously presented) The apparatus of claim 15, wherein the register array further includes:

an exclusive-OR (116) coupled for simultaneously receiving first, second, third and fourth data words stored in the plurality of registers; and

a rotate block (118) having an input coupled to an output of the exclusive-OR and supplying a one bit left circular shift of the data generated by the exclusive-OR to one of the registers in the plurality of registers.

17. (currently amended) The apparatus of claim ~~14~~ 15, wherein an output of the register array is supplied from ~~the~~ a word wise circular queue when computing the second algorithm.

18. (previously presented) The apparatus of claim 14, wherein the first algorithm is an MD5 algorithm and the second algorithm is an SHA-1 algorithm.